UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

MARY THOMAS, individually and on behalf of all others similarly situated, Plaintiff, **v.** **TRUSTEES OF COLUMBIA UNIVERSITY** d/b/a **COLUMBIA UNIVERSITY**, Defendant.	No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Mary Thomas ("Plaintiff"), by and through undersigned counsel, on behalf of herself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against Defendant Trustees of Columbia University d/b/a Columbia University ("Columbia" or "Defendant") upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of counsel as follows:

I. SUMMARY

1. This class action arises out of the recent targeted ransomware attack and data breach ("Data Breach") on Defendant's network that resulted in unauthorized access to the highly sensitive data. As a result of the Data Breach, Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information.

2. Defendant is a higher education institution based in New York offering education services in the United States and throughout the world.[1]

3. As such, Defendant stores a litany of highly sensitive personally identifiable information ("PII")[2] of Plaintiff and Class Members.

4. Upon information and belief, the specific information comprised in the Data Breach includes, but is not limited to, PII, such as name, Social Security number, date of birth, address, telephone number, and email address.

5. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect stop, or mitigate breaches of its systems, thereby allowing cybercriminals unrestricted access to Plaintiff and Class Members' PII.

6. As a result of the Data Breach, Plaintiff and Class Members suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of, and diminution in, value of their personal information.

7. In addition, Plaintiff's and Class Members' sensitive PII —which was entrusted to Defendant— was compromised and unlawfully accessed due to the Data Breach. This information, while compromised and taken by unauthorized third parties, remains also in the possession of

[1] *Overview*, COLUMBIA UNIVERSITY LINKEDIN, https://www.linkedin.com/school/columbia- university/about/ (last visited July 7, 2025).

[2] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the Data Breach.

Defendant, and without additional safeguards and independent review and oversight, remains vulnerable to future cyberattacks and theft.

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect victims' PII.

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party.

10. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant's computer network in a condition vulnerable to cyberattacks.

11. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant and entities like it, and Defendant was thus on notice that failing to take steps necessary to secure the PII against those risks left that property in a dangerous condition and vulnerable to theft. Defendant was further on notice of the severe consequences that would result to Plaintiff and Class Members from its failure to safeguard their PII.

12. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff and Class members' PII; failing to take standard and reasonably available

steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members prompt notice of the Data Breach.

13. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the PII. Had Defendant properly monitored its computer network and systems, it would have discovered the intrusion sooner, as opposed to letting cyberthieves roam freely in Defendant's IT network for months or even years.

14. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

15. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

16. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

17. Plaintiff and Class Members will incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

18. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

19. Accordingly, Plaintiff brings claims on behalf of herself and the Class for: (i) negligence, (ii) breach of implied contract; (iii) invasion of privacy; (iv) breach of fiduciary duty; and (v) violation of New York Deceptive Trade Practices Act ("GBL"). Through these claims, Plaintiff seeks, *inter alia*, damages and injunctive relief, including improvements to Defendant's data security systems and integrated services, future annual audits, and adequate credit monitoring services.

II. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The exact number of class members is unknown to Plaintiff, but upon information and belief exceeds 100, and at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, namely Plaintiff a citizen of Georgia. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. This Court has personal jurisdiction over Defendant Trustees of Columbia University d/b/a Columbia University because its principal place of business is in New York, and it does a significant amount of business in New York.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant Trustees of Columbia University d/b/a Columbia University has its principal place of business located in this District, and a substantial part of the events giving rise to this action occurred in this District.

III. PARTIES

Plaintiff Mary Thomas

23. Plaintiff Mary Thomas is an individual resident and citizen of Memphis, Tennessee.

24. Based on representations made by Defendant, Plaintiff believed Defendant implemented and maintained reasonable security to protect her Private Information.

25. If Plaintiff had known that Defendant would not adequately protect her PII, she would not have allowed Defendant to maintain this sensitive PII.

Defendant Trustees of Columbia University d/b/a Columbia University

26. Defendant Trustees of Columbia University d/b/a Columbia University is a non-profit corporation organized under the laws of New York with its principal place of business at West 116 Street and Broadway, New York, NY 10027.

IV. FACTUAL ALLEGATIONS

Defendant's Business

27. Defendant touts itself as "a leader in higher education in the nation and around the world" for more than 250 years.[3] In 2024, there were approximately 35,769 students enrolled at Columbia.[4]

28. Defendant collects personally identifiable information in the course of doing business. This personally identifiable information includes the PII which was compromised in the Data Breach alleged herein.

[3] Overview, COLUMBIA UNIVERSITY LINKEDIN, https://www.linkedin.com/school/columbia-university/about/ (last visited July 7, 2024).
[4] *Id*.

29. Defendant acknowledges the benefits it receives in collecting this information, stating in its "Information Security Charter" that "[s]uch information is an important resource of the University and any person who uses the information collected by the University has a responsibility to maintain and protect this resource."[5]

30. Upon information and belief, Defendant promises to maintain the confidentiality of Plaintiff's and Class Members' Private Information to ensure compliance with federal and state laws and regulations, and not to use or disclose Plaintiff's and Class Members' Private Information for non-essential purposes.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

32. Defendant recognizes these duties, declaring in its "Information Security Charter" that:

a. "Federal and state laws and regulations, as well as industry standards, also impose obligations on the University to protect the confidentiality, integrity and availability of information relating to faculty, staff, students, research subjects and patients;"

b. "In addition, terms of certain contracts and University policy require appropriate safeguarding of information;" and

c. "The mission of the Information Security Program is to protect the confidentiality, integrity and availability of University Data. Confidentiality means that information

[5] *Information Security Charter*, COLUMBIA UNIVERSITY, https://universitypolicies.columbia.edu/content/information-security-charter (last visited July 7, 2025).

is only accessible to authorized users. Integrity means safeguarding the accuracy and completeness of University Data and processing methods."[6]

33. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members would not have entrusted Defendant with their Private Information had they known that Defendant would fail to implement industry standard protections for that sensitive information.

34. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

35. Additionally, Defendant's policy fir "Handling Personally Identifying Information-PII" states:

a. "Stolen PII is frequently used to commit identity theft and fraud, and should be guarded carefully. Hackers and malware will search a compromised computer for SSN's they can find;"

b. "As a matter of good practice, you should never keep any unprotected PII on your workstation. For Columbia employees and equipment, any PII should be protected with strong encryption or removed;"

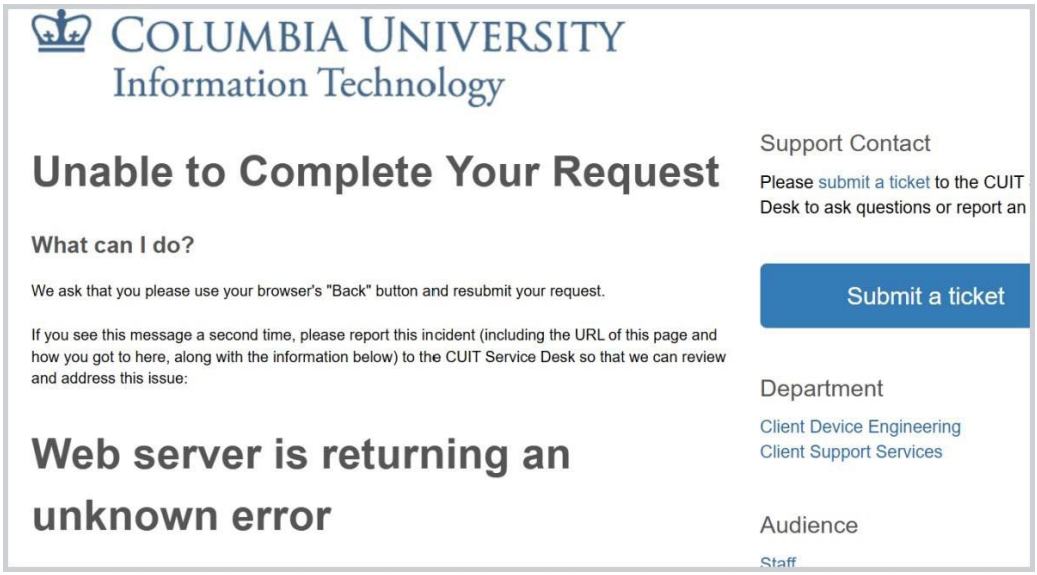
c. "The capture, storage and retention of confidential and sensitive information by CUIT employees is permissible only if it is a University business requirement and complies with Columbia University's Social Security Number Usage Policy, Data

[6] *Id*.

Classification Policy and University Requirements for Endpoints Containing Sensitive Data Policy."[7]

The Attack and Data Breach

36. On June 24, 2025, Defendant announced that it was investigating "widespread system outages" affecting its online platforms.[8]

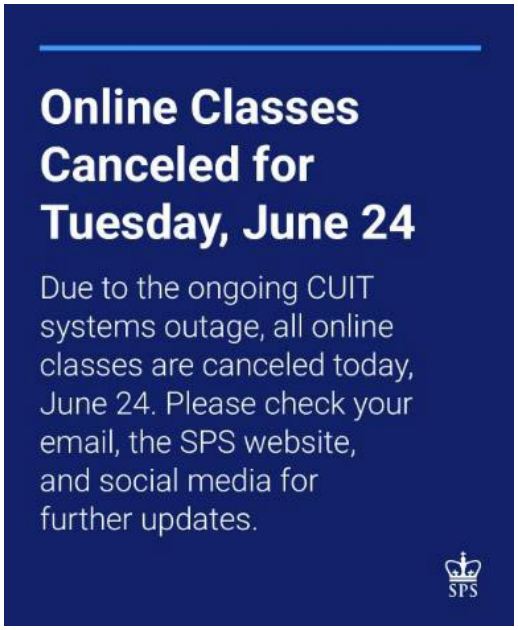


[7] *Handling Personally Identifying Information – PII*, COLUMBIA UNIVERSITY, https://www.cuit.columbia.edu/handling-pii (last visited July 7, 2025).
[8] *Columbia University hit in suspected cyberattack, systems down*, CYBERNEWS, https://cybernews.com/news/columbia-university-suspected-cyberattack-systemwide-outage/ (last visited July 7, 2025).

37. At around 7:30 a.m. E.T. on June 24, 2025, Columbia University Information Technology informed the Columbia community via email of the widespread outages.[9]

38. The outage caused some of Columbia's key services to be offline and inaccessible to both students and professors for an extended period.[10] These included email services, the coursework/assignment platform, and "UNI" authentication service, which students use to log into university accounts.[11]

39. Additionally, as a result of the Incident, Defendant urged professors to make alternative arrangements for class[12] and certain online classes were even canceled on June 24, 2025.[13]



[9] *Columbia, NYPD investigating hourslong University IT outage*, COLUMBIA SPECTATOR, https://www.columbiaspectator.com/news/2025/06/24/columbia-nypd-investigating-hourslong- university-it-outage/ (last visited July 7, 2025).
[10] *Id*.
[11] *Id*.
[12] *Columbia University investigating cyber incident after tech outages*, THE RECORD, https://therecord.media/columbia-university-technology-outages (last visited July 7, 2025).
[13] @columbiasps, Instagram (June 24, 2025) https://www.instagram.com/p/DLTAoPUMe0e/ (last visited July 7, 2025).

40. Defendant reported the incident to the FBI and stated that it is investigating alongside law enforcement, including the New York Police Department.[14]

41. Concerningly, in a statement to Columbia's school newspaper, Defendant confirmed that it was "aware of online posts from a group claiming responsibility for this outage."[15] Though Defendant has since attempted to discredit these claims, experts still believe the outages were the result of a cyberattack.[16]

42. Additionally, during the outages, University officials reported that several screens throughout campus began displaying images "unrelated to University activities," indicating that an unauthorized actor had gained access to these systems and posted the images.[17]

43. Worryingly, this incident is only part and parcel of Defendant's pattern of negligent data security. In May 2024, The Cyber Express, a cybersecurity news site, reported that a cybercriminal group claimed credit for a cyberattack on Columbia.[18]

44. Additionally, in 2007, Columbia exposed 2,600 Social Security numbers belonging to its undergraduate students and alumni.[19] As a result of this security breach, Defendant sent letters to affected students and alumni, encouraging them to monitor their credit to guard against identity theft.[20] These previous incidents further evidence Defendant's lack of adequate cybersecurity measures.

---

[14] *Columbia, NYPD investigating hourslong University IT outage*, COLUMBIA SPECTATOR, https://www.columbiaspectator.com/news/2025/06/24/columbia-nypd-investigating-hourslong- university-it-outage/ (last visited July 7, 2025).
[15] *Id.*
[16] *Major Outage Brings Columbia University to a Standstill*, NEWSINTERPRETATION, https://newsinterpretation.com/columbia-university-hit-by-widespread-digital-outage/ (last visited July 7, 2025).
[17] *Potential Cyberattack Scrambles Columbia University Computer Systems*, THE NEW YORK TIMES, https://www.nytimes.com/2025/06/25/nyregion/columbia-university-cyberattack.html (last visited July 7, 2025).
[18] *Hacktivists Claim Cyberattack on Columbia University After Police Crackdown on Protests*, THE CYBER EXPRESS, https://thecyberexpress.com/cyberattack-on-columbia-university/ (last visited July 7, 2025).
[19] *Data Leak Puts 2,600 at Risk*, COLUMBIA SPECTATOR ARCHIVE, http://spectatorarchive.library.columbia.edu/?a=d&d=cs20070418-01.2.5&srpos=1&e= (last visited July 7, 2025).
[20] *Id*.

45. Due to Defendant's inadequate security measures, Plaintiff and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

46. Upon information and belief, the PII was not encrypted prior to the data breach.

47. Upon information and belief, the cyberattack was targeted at Defendant as a company that collects and maintains valuable personal and financial data, including Plaintiff and Class Members.

48. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and Class Members.

49. Defendant had obligations to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

50. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

51. Upon information and belief, Defendant made promises to Plaintiff and Class members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information, including through "Information Security Charter." [21]

The Data Breach Was Foreseeable and the Defendant Was Aware of Its Risk

52. It is well known that PII, including Social Security numbers and names in particular are invaluable commodities and a frequent target of hackers.

[21] *Information Security Charter*, COLUMBIA UNIVERSITY, https://universitypolicies.columbia.edu/content/information-security-charter (last visited July 7, 2025).

53. In 2023, a record 3,205 data breaches occurred in the United States, resulting in about 349,221,481 sensitive records being exposed, a greater than 100% increase from 2019.[22]

54. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

55. Individuals are particularly concerned with protecting the privacy of their Social Security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their Social Security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[23]

56. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), and, in light of the recent data breaches Wells Fargo has suffered, Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

57. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

---

[22] ITRC (Identity Theft Resource Center), *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last accessed July 7, 2025).

[23] *See* Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed July 7, 2025).

58. Despite the prevalence of public announcements of data breach and data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

Defendant Had A Duty to Plaintiff and Class Members to Secure Private Information

59. At all relevant times, Defendant had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when Defendant became aware that their PII may have been compromised.

60. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and the Class Members, on the other hand.

61. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

62. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

63. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[24] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[25]

The ramifications of Defendant's failure to keep PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Personally Identifiable Information

64. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200,

[24] 17 C.F.R. § 248.201 (2013).
[25] *Id.*

and bank details have a price range of $50 to $200.[26] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[27]

65. As a growing number of federal courts have begun to recognize the loss of value of PII as a viable damages theory, the sale of PII from data breaches, as in the Data Breach alleged herein, is particularly harmful to data breach victims – especially when it takes place on the dark web.

66. The dark net is an unindexed layer of the internet that requires special software or authentication to access.[28] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[29] This prevents dark web marketplaces from being easily identifiable to authorities or those not in the know.

67. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at

---

[26] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: **https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/** (last accessed July 7, 2025).

[27] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: **https://www.privacyaffairs.com/dark-web-price-index-2021/** (last accessed July 7, 2025).

[28] *What Is the Dark Web?,* Experian, *available at* **https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/** (last accessed July 7, 2025).

[29] *Id.*

issue here.[30] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth and medical information.[31] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others." [32]

68. Plaintiff and Class Members' PII is a valuable commodity, a market exists for Plaintiff and Class Members' PII (which is why the Data Breach was perpetrated in the first place), and Plaintiff and Class Members' PII is being likely being sold by hackers on the dark web (as that is the *modus operandi* of data thieves) – as a result, Plaintiff and Class Members have lost the value of their PII, which is sufficient to plausibly allege injury arising from a data breach.

69. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[33] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[34][35]

[30] *What is the Dark Web?* – Microsoft 365, *available at* **https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web** (last accessed July 7, 2025).
[31] *Id.*; *What Is the Dark Web?,* Experian, *available at* **https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/**(last accessed July 7, 2025).
[32] *What is the Dark Web?* – Microsoft 365, *available at* **https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web** (last accessed July 7, 2025).
[33] **https://www.latimes.com/business/story/2019-11-05/column-data-brokers** (last accessed July 7, 2025).
[34] **https://datacoup.com/** (last accessed July 7, 2025).
[35] **https://digi.me/about-us** (last accessed July 7, 2025).

Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[36]

70. The PII stolen in this specific Data Breach was particularly harmful. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

71. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

72. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[37]

73. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

[36] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed July 7, 2025).
[37] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: **https://www.ssa.gov/pubs/EN-05-10064.pdf** (last accessed July 7, 2025).

74. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[38]

75. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[39]

76. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[40]

77. Given the nature of Defendant's Data Breach, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

78. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

[38] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), **http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft** (last accessed July 7, 2025).
[39] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), **http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html** (last accessed July 7, 2025).
[40] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

breach, because credit card victims can cancel or close credit and debit card accounts.[41] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers and dates of birth).

79. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures.

Plaintiff's Experience

80. Plaintiff was required to provide and did provide her PII to Defendant as a condition of applying to enroll.

81. To date, Defendant has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach particularly given the fact that Plaintiff's PII has already been "impacted" in the Data Breach and likely been made available on the dark web to anyone wishing to purchase it.

82. Defendant has not compensated Plaintiff and Class Members for the time they will spend monitoring their accounts, placing credit freezes and fraud alerts, changing online passwords and other actions.

83. Plaintiff and Class Members have been further damaged by the compromise of their PII in the Data Breach which was "impacted" and is in the hands of cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the PII.

84. Plaintiff typically takes measures to protect her PII and is very careful about sharing her PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

---

[41] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed July 7, 2025).

85. Plaintiff stores any documents containing her PII in a safe and secure location, and he diligently chooses unique usernames and passwords for her online accounts.

86. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. In response to the Data Breach, Plaintiff has spent significant time monitoring her accounts and credit score, changing her online account passwords and verifying the legitimacy of the Notice and researching the Data Breach. This is time that was lost and unproductive and took away from other activities and duties.

87. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her PII — a form of intangible property that she entrusted to Defendant for the purpose of applying to enroll, which was compromised in and as a result of the Data Breach.

88. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

89. Plaintiff suffered emotional distress and increased stress and anxiety as a result of the Data Breach because of the actions he has been forced to undertake, the loss of control over her most intimate information, and the fact that he must remain vigilant for the remainder of her life.

90. Plaintiff has suffered imminent and impending injury arising from the increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

91. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff as a condition of applying to enroll. Plaintiff, however, would not

have entrusted her PII to Defendant had she known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

92. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ACTION ALLEGATIONS

93. Plaintiff brings this suit on behalf of herself and a class of similarly situated individuals under Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, which is preliminarily defined as:

> All individuals whose PII was accessed and/or acquired by an unauthorized party in the Data Breach (the "Class").

94. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

95. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, thousands of individuals have been affected by this breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

96. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

i. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

iv. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

v. Whether Defendant owed a duty to Class Members to safeguard their PII;

vi. Whether Defendant breached its duty to Class Members to safeguard their PII;

vii. Whether computer hackers obtained Class Members' PII in the Data Breach;

viii. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

ix. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

x. Whether Defendant's conduct was negligent; and;

xi. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

97. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

98. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

99. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

100. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

101. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

102. Likewise, particular issues under Federal Rule 23(c)(4) are appropriate for

certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

xii. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

xiii. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

xiv. Whether Defendant's failure to institute adequate protective security measures amounted to negligence; and

xv. Whether Defendant failed to take commercially reasonable steps to safeguard PII,

103. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

104. Plaintiff hereby repeats and realleges paragraphs 1 through 103 of this Complaint and incorporates them by reference herein.

105. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII for pecuniary gain, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

106. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

107. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed. The harm that Plaintiff and Class Members experienced was within the zone of foreseeable harm known to Defendant.

108. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between each Defendant and Plaintiff and the Class. Specifically, Defendant actively solicited and gathered PII as part of its business and was solely responsible for and in the position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a resulting data breach.

109. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

110. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices and the frequency of data breaches in general.

111. Defendant also had a common law duty to prevent foreseeable harm to others. Plaintiff and the Class were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems. It was foreseeable that Plaintiff and Class members would be harmed by the failure to protect their

personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

112. Defendant's conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class's PII, including basic encryption techniques available to Defendant.

113. Plaintiff and the Class had and have no ability to protect their PII that was in, and remains in, Defendant's possession.

114. Defendant was in a position to effectively protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

115. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

116. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within Defendant's possession.

117. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

118. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

119. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

120. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), Defendant had a separate and independent duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

121. The FTCA is intended, in part, to protect individuals whose PII is maintained by another and who are unable to safeguard their information as they cannot exercise control or direction over the data security practices.

122. Plaintiff and the members of the Class are within the class of persons that the FTCA was intended to protect as their PII was collected and maintained by Defendant and they were unable to exercise control over Defendant's data security practices.

123. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against.

124. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the members of the Class.

125. Defendant breached its duties to Plaintiff and the members of the Class under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

126. Had Plaintiff and the members of the Class known that Defendant would not adequately protect their Private Information, Plaintiff and the members of the Class would not have entrusted Defendant with their Private Information.

127. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

128. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the members of the Class, they would not have been injured.

129. The injury and harm suffered by Plaintiff and the members of the Class was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiff and the members of the Class to experience the foreseeable harms associated with the exposure of their Private Information.

130. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and

future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

131. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

132. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

133. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class are now at an increased risk of identity theft or fraud.

134. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff is entitled to and demands actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

135. Plaintiff hereby repeats and realleges paragraphs 1 through 103 of this Complaint and incorporates them by reference herein.

136. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

137. At the time Defendant acquired the PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

138. Implicit in the agreements between Plaintiff and Class Members and Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

139. Plaintiff and the Class would not have entrusted their PII to Defendant had they known that Defendant would make the PII internet-accessible, not encrypt sensitive data elements, and not delete the PII that Defendant no longer had a reasonable need to maintain it.

140. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

141. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

142. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

143. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT III
INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

144. Plaintiff hereby repeats and realleges paragraphs 1 through 103 of this Complaint and incorporates them by reference herein.

145. Plaintiff and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access, as occurred with the Data Breach.

146. Plaintiff and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

147. Defendant intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party. Defendant's acts and omissions giving rise to the Data Breach were intentional in that the decisions to implement lax security and failure to timely notice Plaintiff and the Class were undertaken willfully and intentionally.

148. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

149. This invasion of privacy resulted from Defendant's intentional failure to properly secure and maintain Plaintiff's and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded and private data.

150. Plaintiff's and Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiff's and Class Members'

PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

151. The disclosure of Plaintiff's and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

152. Defendant's willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiff's and Class Members' sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

153. The unauthorized access, exfiltration, and disclosure of Plaintiff's and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

154. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT IV
UNJUST ENRICHMENT/QUASI CONTRACT
(On Behalf of Plaintiff and the Class)

155. Plaintiff hereby repeats and realleges paragraphs 1 through 103 of this Complaint and incorporates them by reference herein.

156. This Count is brought in the alternative to Count II, Breach of Implied Contract.

157. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. In so conferring this benefit, Plaintiff and Class Members understood that part of the benefit Defendant derived from the PII would be applied to data security efforts to safeguard the PII.

158. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

159. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

160. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

161. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

162. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

163. Plaintiff and Class Members have no adequate remedy at law.

164. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how

to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

165. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

166. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT IV
VIOLATION OF NEW YORK DECEPTIVE TRADE PRACTICES ACT ("GBL")
New York Gen. Bus. Law § 349
(On Behalf of Plaintiff and the Class)

167. Plaintiff hereby repeats and realleges paragraphs 1 through 103 of this Complaint and incorporates them by reference herein.

168. Under the New York Gen. Bus. Law § 349, "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

169. Notably, Defendant's deceptive acts and/or practices were directed at consumers. After all, via its policies, Defendant represented to consumers that they would, *inter alia*, use reasonably adequate data security.

170. And these deceptive acts—including the quotations provided *supra*—were materially misleading insofar as they induced consumers to rely on such statements and disclose their PII.

171. Section § 349 applies to Defendant because there is a sufficient nexus between Defendant's conduct and New York. After all, Columbia University is incorporated in New York and its corporate headquarters is in New York, New York.

172. And, upon information and belief, the misleading acts and/or practices alleged herein—including the manifestations in Defendant's data security policies—were written, approved, and/or otherwise authorized by Defendant within the state of New York.

173. In particular, Defendant violated Section § 349 by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

174. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII.

175. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

176. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII that Plaintiff and Class members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

177. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class members' rights.

178. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for

fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

179. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

180. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class defined herein, prays for judgment as against Defendant as follows:

a.) For an Order certifying this action as a Class action and appointing Plaintiff and her counsel to represent the Class;

b.) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c.) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Breach;

d.) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e.) Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

f.) For an award of actual damages, compensatory damages, statutory damages and statutory penalties, in an amount to be determined, as allowable by law;

g.) For an award of punitive damages, as allowable by law;

h.) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i.) Pre- and post-judgment interest on any amounts awarded and,

j.) All such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury.

DATED: July 7, 2025

Respectfully submitted,

/s/ Steven Sukert

Steven Sukert (NY Bar #5690532)
Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 525-4100
sukert@kolawyers.com
ostrow@kolawyers.com

Attorneys for Plaintiff and the Putative Class

**Pro Hac Vice* application forthcoming